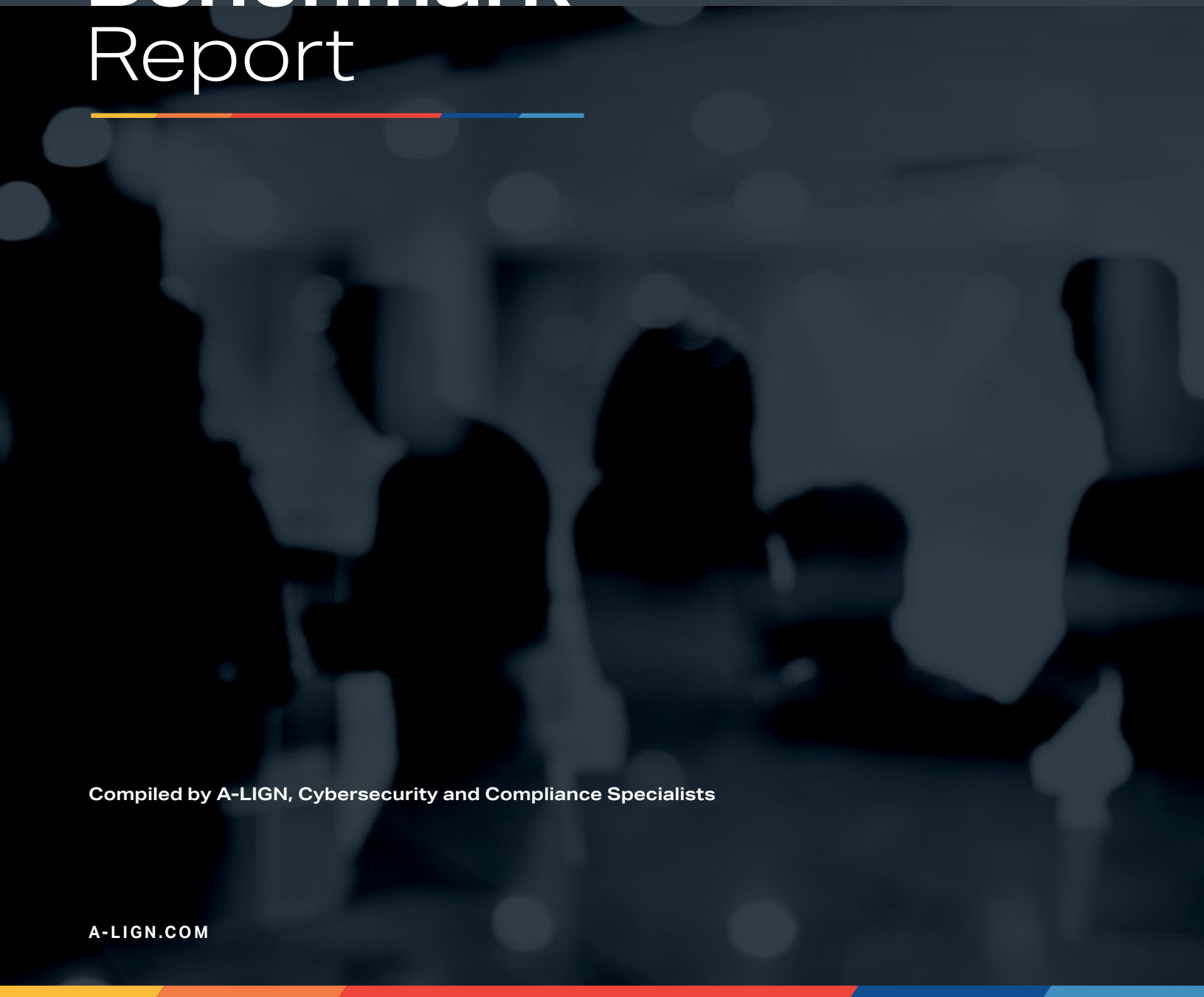
A-LIGN

2021 **Compliance Benchmark** Report



Compiled by A-LIGN, Cybersecurity and Compliance Specialists

A-LIGN.COM

2021 **Compliance Benchmark** Report

Organizations today operate in an increasingly complicated and competitive global marketplace.

Consumers, businesses, and governments are becoming more aware of privacy issues and cybersecurity threats. Meanwhile, business is increasingly international, and remote work is becoming more common across industries, especially during the COVID-19 pandemic. At the same time, cybersecurity risks are growing, with breaches hitting high-profile targets constantly.

Take, for example, one of the most sophisticated and widespread attacks to date: the SolarWinds supply chain attack. Carried out over several months, this attack impacted 100 companies and nine U.S. federal agencies, according to a February 2021 article in The Verge.

An Increasingly Complex Compliance Landscape

Faced with demand from customers and partners for assurances that sensitive data will be protected across corporate boundaries, as well as regulatory pressures to address privacy and cybersecurity risks such as the General Data Protection Regulation (GDPR) or the California Privacy Regulation Act (CPRA), organizations often find themselves pursuing an increasing number of compliance programs.

These compliance programs are growing in scope and complexity. They must cover regulatory mandates and voluntary frameworks that demonstrate business maturity, such as:

- System and Organization Controls (SOC) 1 and 2
- International Organization for Standardization (ISO) frameworks, such as ISO 27001
- The U.S. Health Insurance Portability and Accountability Act (HIPAA)
- The Federal Risk and Authorization Management Program (FedRAMP)
- The Payment Card Industry Data Security Standard (PCI DSS)
- HITRUST Common Security Framework (CSF)
- And more

Meanwhile, new regulations and frameworks are on the horizon, such as the U.S. Cybersecurity Maturity Model Certification (CMMC).

Adapting to COVID-19

Of course, 2020 was also a year marked by the COVID-19 pandemic. Organizations of all sizes had to quickly adapt to distributed workforces and make huge shifts in corporate operations—not to mention new threats seeking to take advantage of those changes. Faced with the rise of remote work, diverse departments had to find new ways to complete their work from numerous locations and home offices, while security professionals scrambled to protect them.

IT and cybersecurity teams were already accustomed to using technology to integrate tools, automate processes, and improve collaboration. The COVID-19 pandemic only accelerated these trends, and compliance teams were faced with the same challenge—how to keep audits on track with teams scattered across locations.

Introducing the 2021 Compliance Benchmark Report

In this ever-changing business and compliance landscape, you may be wondering: How can my organization stay on top of compliance requirements?

In A-LIGN's first Compliance Benchmark Report, we asked over 200 cybersecurity, IT, quality assurance (QA), internal audit, finance, and other professionals about their compliance programs. We asked about their organizations, how they run their programs, and the impact of the COVID-19 pandemic on their compliance plans.

In this report, we're bringing together a benchmark by industry to see where your organization stands, an analysis of key findings, and a set of best practices that any organization can use to improve their compliance program in 2021 and beyond.

Contents

Survey Methodology

The survey was administered by A-LIGN via SurveyMonkey between November 2020 and February 2021.

Respondents' titles included CEO or president, other C-level executives, vice presidents, directors, or managers across the IT/technology, infosec/cybersecurity, QA, internal audit, and finance/accounting departments, among others.

Industries represented include:

- Technology
- IT services
- Professional services
- Media and entertainment
- Healthcare
- Insurance
- Legal
- Retail
- Finance and banking
- Manufacturing and construction
- Government

218 individuals completed the survey in whole or in part.

Results in this report are rounded up or down to the nearest whole percentage.

Benchmark Your Organization

When organizations come to A-LIGN, one of the things they often want to know is: What are my peers doing?

Compliance needs vary by industry, company size, customer profile, geographical footprint, cybersecurity maturity, and many other factors. It can be difficult for organizations to understand whether they are doing enough to ensure compliance with key regulations or important frameworks.

Benchmarking can help guide decisions around questions such as:

- Should I be considering different or new frameworks?
- Are there regulations I'm not aware of?
- Am I doing too many or too few audits?
- Am I behind the curve on compliance?
- Do my peers have a competitive advantage due to their approach?
- And more

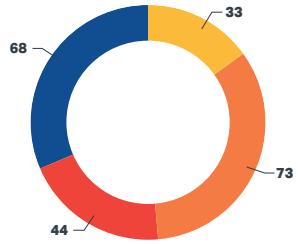
Based on a survey of 218 respondents, A-LIGN compiled the following benchmark data by industry, revenue, and company size. You can use this data to compare various attributes of your compliance program with those of organizations similar to yours.

Benchmark Data

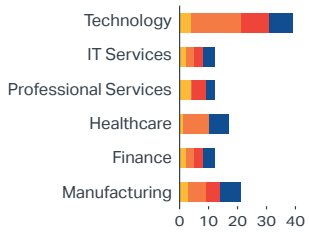
Numbers represents the actual number of respondents who selected that answer.

Number of Audits Conducted Each Year

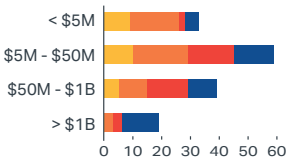
All Responses



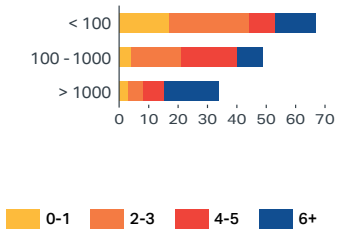
By Industry



By Annual Revenue

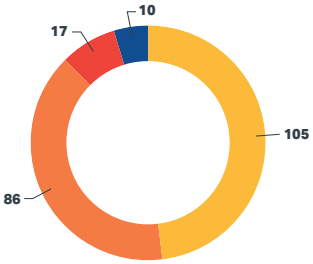


By Company Size

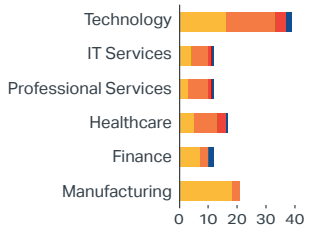


Number of Audit Providers Used

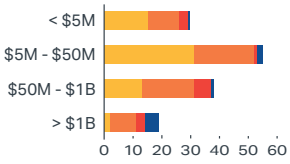
All Responses



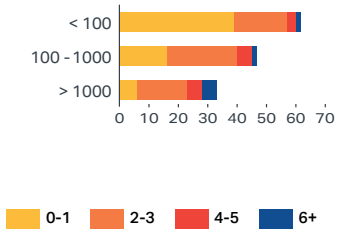
By Industry



By Annual Revenue

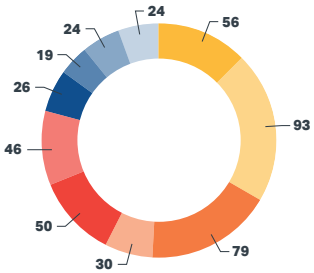


By Company Size

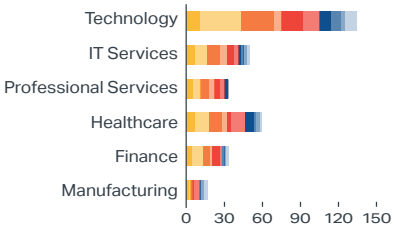


Audits/Assesments Currently Doing or Planned in Next 12 months

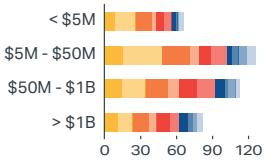
All Responses



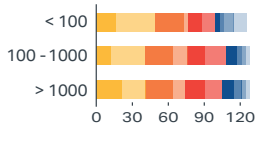
By Industry

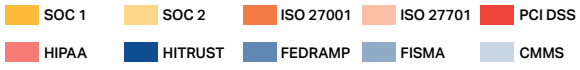


By Annual Revenue



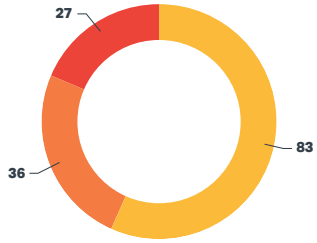
By Company Size



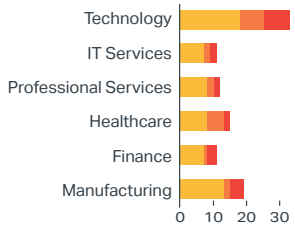


Time Spent Preparing for Audits Annualy

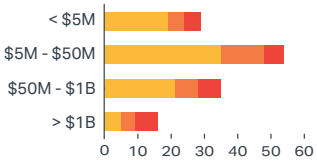
All Responses



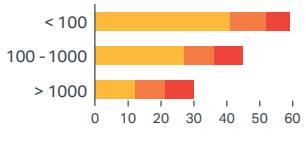
By Industry

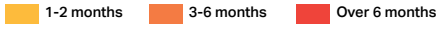


By Annual Revenue



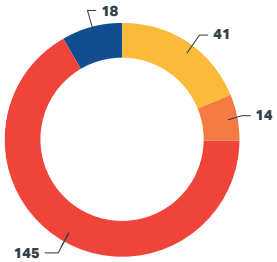
By Company Size



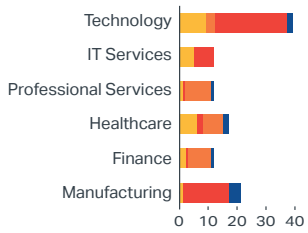


Compliance and Security Software Used to Prepare for Audits

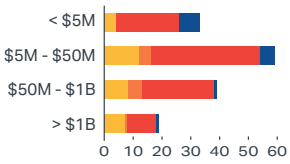
All Responses



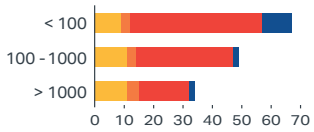
By Industry

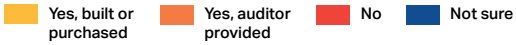


By Annual Revenue



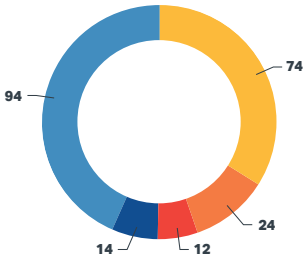
By Company Size



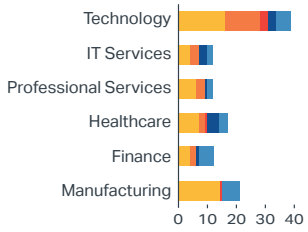


Amount Spent on Audits Annually

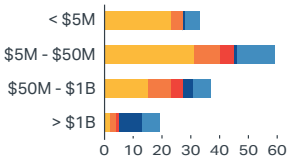
All Responses



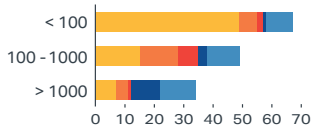
By Industry

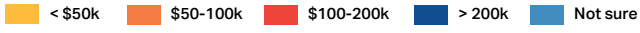


By Annual Revenue



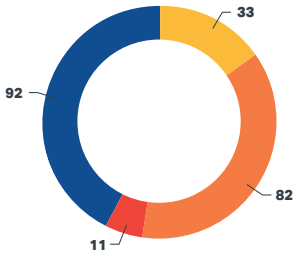
By Company Size



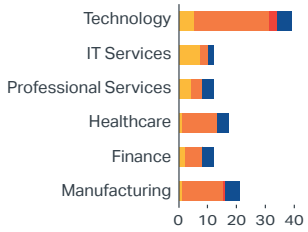


Impact of COVID on Departmental Budget

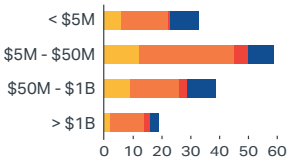
All Responses



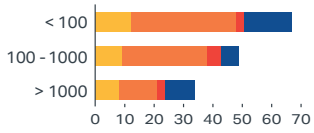
By Industry



By Annual Revenue



By Company Size



Analysis and Key Findings

Our 2021 Compliance Benchmark Report uncovered numerous trends in compliance and the realities facing IT professionals and compliance teams today. These findings offer organizations:

- Insights into common pain points
- Potential practices to adopt
- Ways to make auditing less painful and more strategic

Of course, this report—and the benchmark above—should be viewed through the lens of the COVID-19 pandemic, which generated massive changes and new ways of thinking about work, cybersecurity, and compliance. Businesses were forced to make many shifts, both in how they managed their own workers and how they interacted with customers, partners, investors, and others.

Below, we explore several key trends highlighted in our survey results.

The Pandemic Changed the World in 2020, But Compliance Continued to March Forward

The 2020 pandemic changed workplace norms, corporate processes, and workflows for everyone, and compliance programs also felt the impact of COVID-19. Suddenly, teams had to rethink the audit process completely. Our survey found that the pandemic did not put a halt to audits and assessments. Despite the pandemic, organizations continued to invest in security and complying with key regulations.

We dig into three key pandemic trends below.

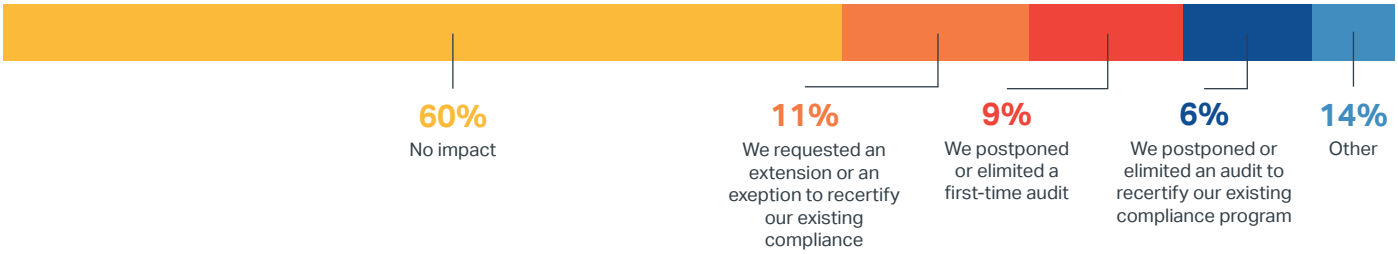
Compliance Programs Stayed Strong

We were curious if the pandemic would curtail compliance programs. After all, many other business functions and departments saw freezes, budget cuts, and halted work. Did compliance programs slow down, too?

Regulations and rules didn't go away with the pandemic, and compliance programs stayed strong despite global circumstances. We found that 85% of companies kept their compliance programs on track. In fact, 60% of respondents said that the pandemic had no impact on their compliance programs.

That said, some respondents did report delays to their compliance programs, with 11% requesting an extension or an exception to recertify an existing program. However, only 6% postponed or eliminated an existing audit to recertify their existing compliance program. This held true for first-time

What was the impact of COVID-19 on your organization's compliance program?



audits, too—a tiny 9% said they'd postponed or eliminated a first-time audit due to COVID-19.

Overall, compliance continued to march forward despite the widespread global pandemic.

COVID-19 Drove Remote Audits

Many audits and assessments involve intense evidence collection and on-site visits from auditors. So what happens when in-person work is banned and travel is restricted?

The COVID-19 pandemic forced other key business functions into a remote environment, and compliance programs were no exception. The majority of survey respondents—a huge 71%—said they have conducted remote audits or are planning to conduct remote audits.

Many of the people contributing to audits and assessments are, in fact, technical people on IT and cybersecurity teams. These employees are typically very good with technology and have already adopted numerous tools for automation, organization, and collaboration. With this rise in remote audits spurred by the pandemic, we see a huge opportunity for compliance teams to leverage tools and technology for more efficient remote auditing processes.

COVID-19 Had a Low Impact on Budgets

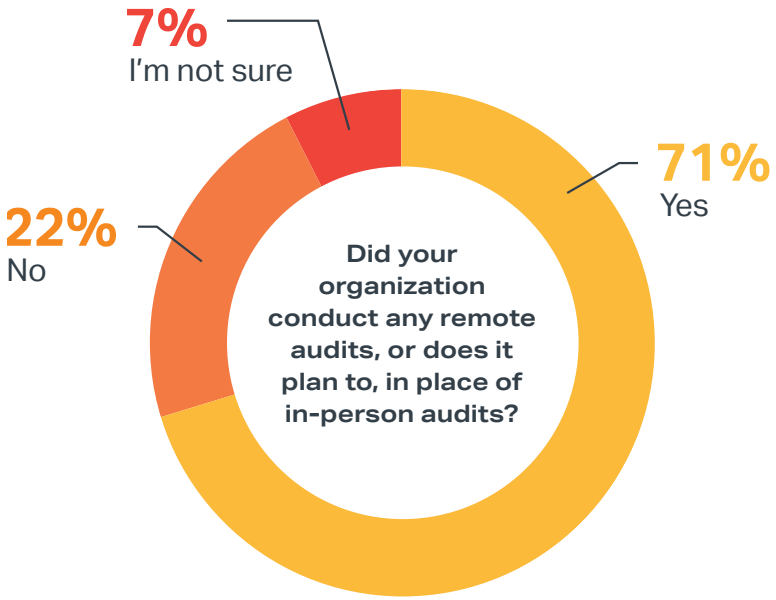
The coronavirus pandemic led to financial struggles for some businesses and industries, and we wondered whether budgets in departments related to compliance had been impacted. Fortunately, our respondents reported that their departmental budgets were largely spared.

65% of respondents familiar with their department budget said COVID-19 had no impact on their budget. This is in keeping with the results mentioned above, which indicate that compliance programs stayed on track despite the pandemic. That said, COVID-19 did not drive growth in departmental spending either—only 9% of respondents saw their budget increase.

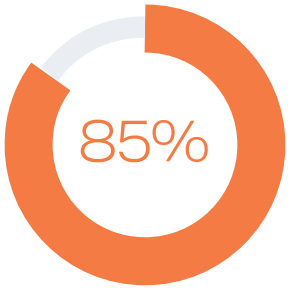
The three trends above affirm A-LIGN's experience working with organizations throughout the pandemic.

Over the past year, we have seen companies become much more capable in remote work settings. They are now more aware of the cybersecurity threats of remote work and what it takes to succeed in remote operations. We've seen better self-enforcement as IT and information security departments step up to the plate to prevent and remediate cybersecurity threats. As pandemic-related cybersecurity concerns have grown, we have also seen growing interest in vendor risk management programs.

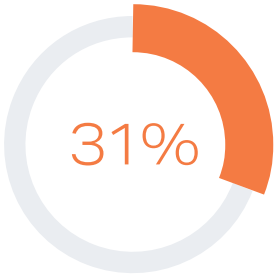
We'll be keeping a close eye on the remote audit trend at A-LIGN to see if it continues into 2021 and beyond. This is something A-LIGN has been supporting clients with during the COVID-19 pandemic. With more technology and tools to support evidence collection, we envision remote audits—either in part or whole—as a lasting trend.



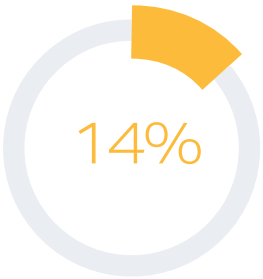
Organizations Conduct Multiple Audits as Disjointed, Redundant Projects



Organizations conduct more than one audit a year



Organizations conduct more than six audits per year



Organizations consolidate audits into a single event

Auditing is often described as a stressful, time-consuming process. Organizations leave audits until the last minute, scrambling to assemble the necessary data close to the deadline for submitting materials. This process creates a whirlwind of chaos for stakeholders, from IT managers to cybersecurity teams and beyond. And it's not much fun for the auditors, either, who come into a process rife with human error, stress, and frustration.

With so much revenue on the line and so many compliance requirements in play, you might think that organizations would make a point of conducting multiple audits in a strategic, unified manner. However, that is not always the case—many compliance assessments and audits are not being strategically planned.

According to our survey data, most organizations complete multiple audits every year. In fact, 85% of respondents conduct more than one audit a year, yet only 14% consolidate audits into a single annual event.

And organizations are doing this many times a year: In fact, 31% of organizations are conducting more than six audits or assessments a year.

Some Industries Consolidate Audits More Than Others

The number of audits varies by industry (healthcare does the most). Additionally, the number of audits correlates closely to the amount of revenue the organization pulls in; most organizations with over $1 billion in revenue are doing more than six audits per year. Interestingly, the inflection point seems to be $5 million in revenue—once companies surpass this point, the number of organizations doing over four audits jumps from 21% for organizations with less than $5 million revenue to 60% for those with greater than $5 million in revenue.

Audit consolidation varied by industry but was least common in healthcare, where 94% of respondents reported multiple, individually-managed audits and assessments. This may be because healthcare, as we saw earlier, tends to do more assessments in general. Also, unlike some other industries, it is highly regulated and needs to meet government mandates. For example, organizations that touch patient data in the U.S. must comply with HIPAA.

Technology companies had the highest rate of consolidated audits at 26%,

a number that still feels remarkably low. However, across industries, most organizations have not consolidated their auditing process—which means they are most likely using resources inefficiently and scrambling at the last minute to execute on chaotic compliance programs.

Audits Cost Organizations Precious Time

Many organizations are juggling multiple, uncoordinated audits, but how much time do teams spend on preparing for an audit?

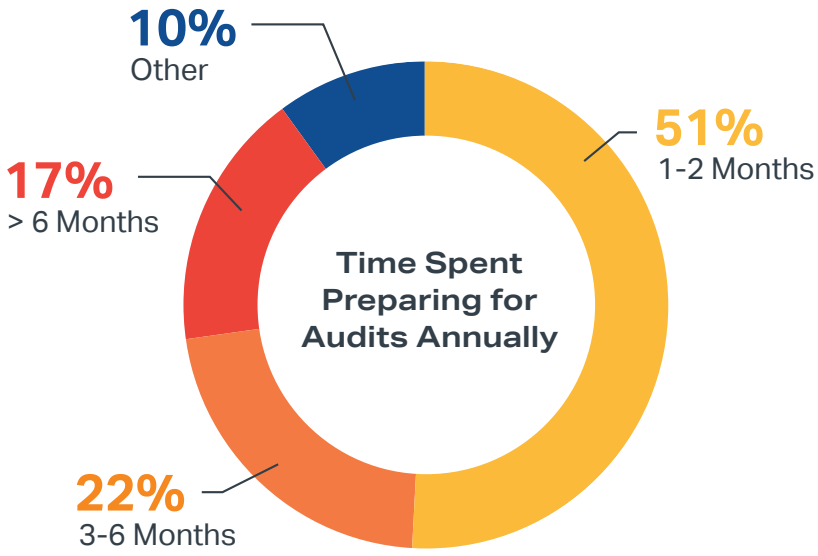
We asked respondents how much time they spent annually on preparing for audits and assessments, including tasks such as:

- Writing policies
- Collecting evidence
- Remediating issues

Unfortunately, it seems that organizations spend significant time preparing for audits and assessments, with 51% of respondents familiar with the audit process spending one to two months on prep each year. This was the most common amount of time spent across companies of all revenue and employee sizes.

Some organizations (17%) even spend upwards of six months preparing for audits and assessments. This happened more often in companies with over $1 billion in revenue, which may be due to having more audits, assessments, and certifications to complete. No matter the case, however, half a year is still an incredibly long amount of time for any individual or team to spend on preparation.

It's not hard to imagine how these preparation timelines could multiply for organizations with numerous, disjoined audits. This is why strategic planning year-round is so important. When organizations meet key controls, continuously collect evidence, automate processes with software, and organize policies throughout the year, preparing for an auditor is a much faster experience. We discuss this further in our best practices section later in this report.



Drivers of Compliance Vary, But Organizations Often Pursue Audits to Win New Business

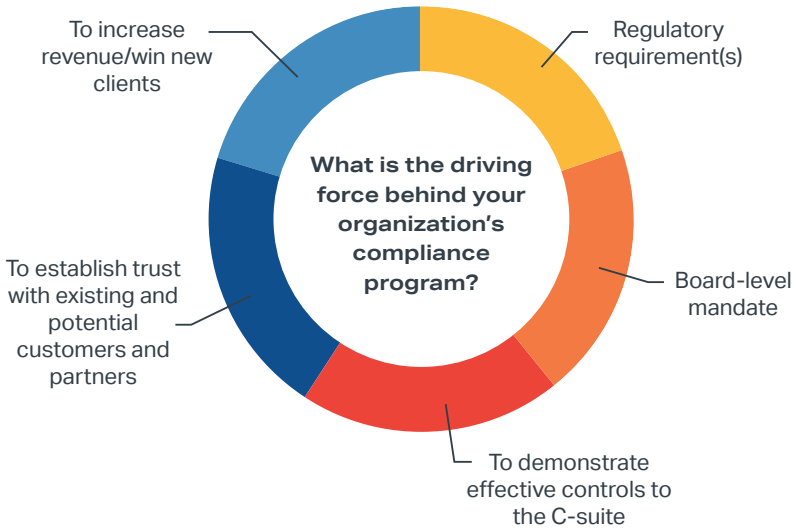
Compliance is a legal necessity in some industries, notably healthcare, financial services, and government contracting. For other industries like technology, complying with frameworks and best practices may be a business benefit or differentiator but is not always legally required.

For example, for companies selling goods to consumers, PCI DSS may be challenging to do business without (because credit card processors require it to process payment card info), but it is not mandated by any government. The same can be said for SOC 2, which is not part of the law and yet is an expected and well-respected certification.

We wanted to know: What drives compliance programs?

We asked respondents to rank their "Most Important" drivers from a list of common pressures. The results varied, and our data did not show a single clear leading cause. Regulatory requirements (19%), meeting board-level mandates (16%), establishing trust with potential and existing customers (15%)—all of these drivers (and others) were clustered together. We were surprised by this, but one plausible explanation is that different individuals, in different functions and levels of an organization, have different perceptions about what is really behind these projects.

Despite the muddled nature of the compliance driver data, our survey did highlight a common benefit that organizations receive from conducting assessments and audits, no matter why they were initiated in the first place: winning new business.



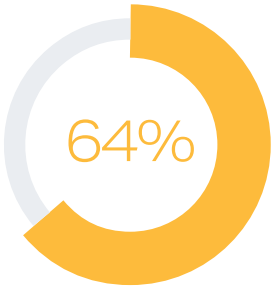
Our data shows 64% of respondents have conducted an audit or assessment to win new business. There were also consequences to not having proper certifications or reports, with 14% of respondents having lost a business deal because they were missing a compliance certification.

This data highlights the way many organizations approach audits: reactively.

In our experience, audits and assessments often come onto an organization's radar when a partner, customer, vendor, or other stakeholder asks for proof of compliance with a framework, such as SOC 1 or 2, during the sales process. They want to see a certification before they'll sign a deal, often to manage their own risk and data security.

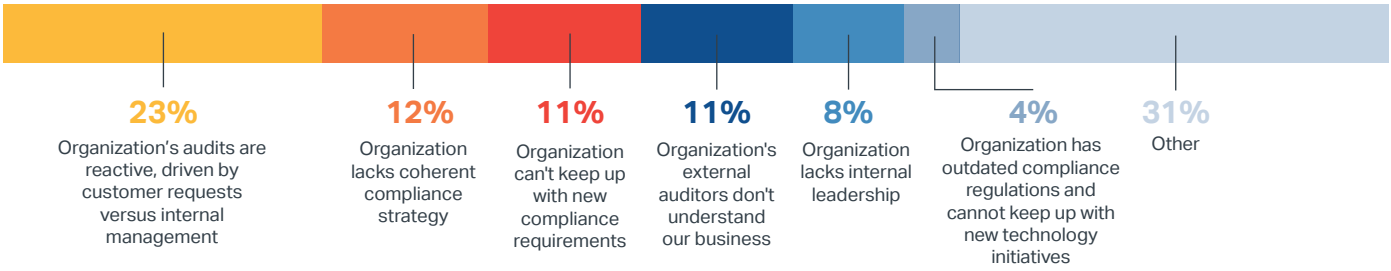
A request comes in—often to a technical IT or cybersecurity manager, not the C-suite or the board of directors—and suddenly it's all hands on deck to complete the assessment or audit. This reactive approach has ramifications for internal teams and causes challenges for organizations. In fact, 23% of respondents stated the greatest challenge to their compliance strategy was their organization's reactive approach to audits driven by customer requests versus internal management priorities. Without a single key driver behind their compliance programs, many organizations lack a strong sense of direction from their leadership teams in this regard.

This isn't to say that executives and boards are unconcerned about regulations or cybersecurity—quite the opposite. With the rise in high-profile hacks, malicious tools such as ransomware, and the growth in remote work, leaders are more aware than ever of the dangers of poor cybersecurity. However, this awareness often doesn't trickle down to a compliance program. The insights above highlight the dichotomy between what boards and regulations require versus how internal teams perceive the resourcing for and strategy behind compliance programs (or lack thereof).



Organizations conducted an audit to win new business

What is the greatest challenge to your compliance strategy?



Audit Automation Isn't Automatic Yet

Across many industries, software is transforming business practices in part through automation. During the COVID-19 pandemic, many business functions embraced the power of technology tools to improve business functions and collaboration in a remote work environment.

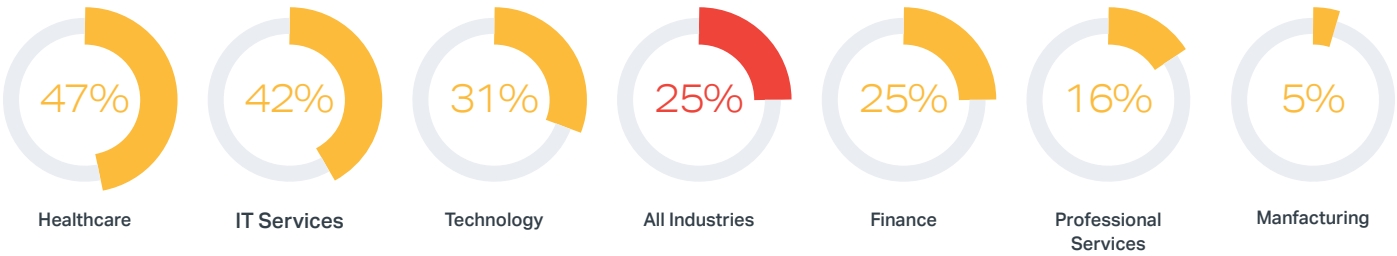
Auditing is ripe for technological disruption, too. There is an increasing number of software solutions specifically designed to help organizations manage the processes, communications, and pieces of evidence necessary to satisfy an audit or third-party assessment.

Yet, despite the growing availability of compliance software and automation, we found that companies are by and large not using these tools.

Only 25% of respondents stated that they are using a software solution to prepare for audits and assessments such as an automated security, compliance, or governance risk compliance (GRC) solution.

By industry, healthcare companies ranked higher than average on technology usage for auditing and assessment (either purchased or developed in-house) at 47%. This may

Percentage of organizations that use a software solution to prepare audits



be due to higher regulation and audits in the healthcare. Also, the higher rate of software adoption in healthcare may be driven by HITRUST requirements and HITRUST's online MyCSF platform. The tech-savvy IT industry came in second at 42%.

While companies with more employees were more likely to use software, an organization's ability to generate more revenue didn't necessarily increase adoption—53% of companies with over $1 billion in revenue still did not use compliance software.

We also found that very few auditors are currently offering technology tools. In fact, only 6% of respondents said they received compliance software from their auditor.

The low adoption rate of compliance software represents a big missed opportunity for organizations. Automation and compliance management software can provide benefits such as:

- Creating efficiencies across multiple audits
- Improving communication between departments and managers, and
- Reducing the amount of employee time required for auditing

In 2021 and beyond, adopting auditing software will be a huge step forward for many organizations. We'll talk about this further in our best practices section later in this report.

SOC 2 is the Most Popular Audit

SOC 2 is a popular framework that many organizations adopt across industries. Created and administered by the American Institute of Certified Public Accountants (AICPA), SOC 2 is designed to ensure that organizations meet a consistent set of privacy and security criteria and have appropriate measures in place to protect information.

Our survey affirmed the popularity of SOC 2, finding that 47% of respondents said SOC 2 was the most important audit, attestation, or assessment for their business. Second to SOC 2, 39% claimed ISO 27001—another important security framework—as most important.

While SOC 2 isn't mandated, it's a strong signifier that an organization manages data and privacy in a professional, process-oriented manner. It builds trust with customers, partners, and others—which is why it is often requested by customers and external stakeholders.

We found that 33% of respondents reported that customers most frequently ask for SOC 2 first. That was followed, again, by ISO 27001 at 22%.

The importance of SOC 2 and ISO 27001 was underscored by respondents' compliance plans for the next 12 months. 43% of total respondents were currently conducting or planning to conduct a SOC 2 audit in the next 12 months, while 36% were doing or planning ISO 27001. SOC 2 was the most in progress and/or planned audit for technology, healthcare, and finance organizations. Notably, technology organizations stood out as strong demand leaders for SOC 2, with a whopping 82% doing or planning to do SOC 2. Meanwhile, IT ranked highest for doing ISO 27001 at 83%.

Audits Currently Doing or Planned in Next 12 Months

Organizations Struggle with Staffing and Evidence Collection

At A-LIGN, we often hear that auditing and assessing can be a stressful experience.

When audits are reactive—versus proactively managed as a strategic initiative—teams may feel like they've been thrown a ticking time bomb. They rush to gather evidence and organize themselves before an auditor comes into the picture. And often, there's a different auditor for each unrelated audit, which can lead to duplicated work and other challenges.

Respondents reported several challenges that made the auditing process difficult:

- Limited Staff: 44% of respondents named limited staff resources dedicated to compliance as their greatest challenge.
- Challenges in Evidence Collection: 27% pointed to tedious and manual evidence collection. (Which is perhaps unsurprising given our findings that most organizations aren't using technology to ease the process).
- Lack of Budget: Close to 10% called out budget constraints as a top challenge to their compliance program efforts.

We don't find it surprising that organizations struggle with staff time and evidence collection, especially since most are not consolidating audits or using compliance management technology to streamline processes. Employees already strapped for time don't have the bandwidth to prepare for an audit—and the one to two months that 51% of knowledgeable respondents reportedly spend on audit

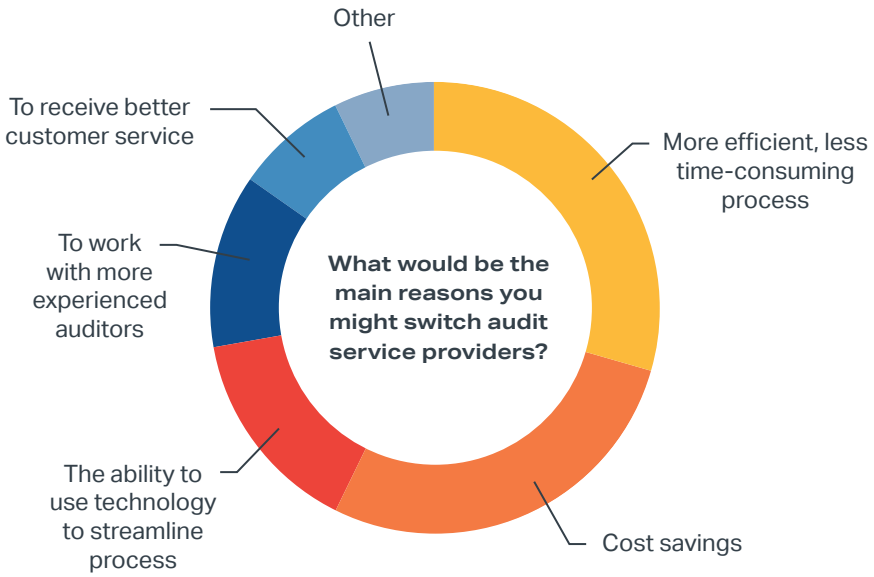
What is the greatest challenge of your audit process?

preparation annually is a considerable amount of time out of their schedules.

Also, imagine the strain of the COVID-19 pandemic in 2020. Already overwhelmed and most likely working from home, it's fair to assume that employees struggled even more to collect evidence and communicate about audits and assessments. Given these factors, it's natural that respondents feel constrained in terms of staff and budget and feel burdened by evidence collection.

When the right technology is paired with a strategic plan, organizations can become more efficient at preparing for audits and assessments. Compliance management software could help reduce the amount of time organizations spend preparing for audits and assessments—which alleviates pressures on staffing shortages and makes evidence collection easier.

The challenges noted above—staffing, evidence collection, and budget—underscore that it takes time, resources, a thoughtful strategy, and the right partners to ensure a smooth auditing experience. Our survey results support this; 46% said they would switch auditors for a more efficient and less time-consuming process. Organizations are also seeing the benefits of technology for more efficient auditing, and 23% of respondents would change auditors for technology that streamlines the auditing process.



Privacy Laws are Having an Impact on Compliance Programs

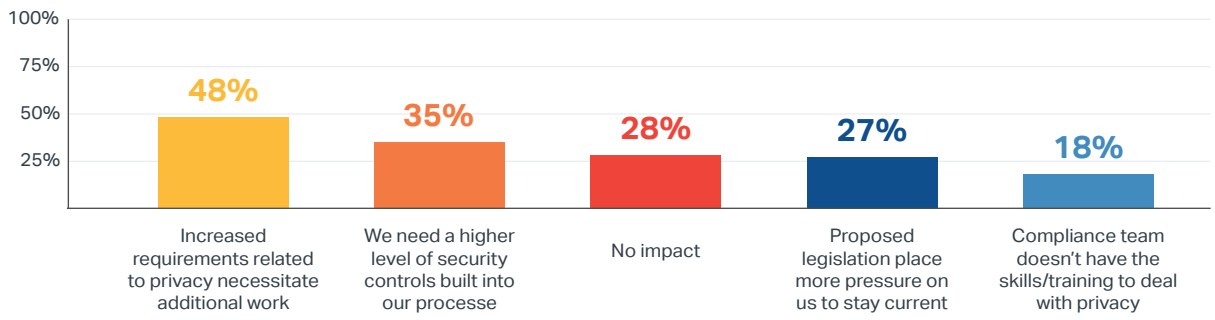
From the EU's GDPR and California's CCPA to up-and-coming legislation in Virginia and other U.S. states, privacy is at the forefront of regulators' minds. And it's not just regulators—consumers are concerned about their privacy and data.

An impressive 71% of respondents said that privacy regulations had an impact on their compliance practices. Many noted that increased requirements and upcoming legislation are driving these changes—48% said that growing privacy requirements are necessitating additional work, while 27% said that proposed legislation is pressuring them to stay more current.

As awareness around privacy grows, organizations are looking to incorporate more privacy controls into their compliance programs. In our survey, 35% of respondents noted that they needed higher levels of security controls. This trend is only likely to continue, as COVID-19 has driven an increase in remote work and generated new cybersecurity and privacy concerns.

GDPR remains the gold standard for privacy, and much of the new legislation coming into existence borrows heavily from it. That said, organizations face a patchwork of laws in the U.S. and globally. As more national, regional, and local governments turn their attention to privacy, we predict that organizations will continue to evolve their compliance programs to match.

What impact has the increased focus on privacy had on your compliance practice and audits?



Five Best Practices for Compliance Management

Our 2021 Compliance Benchmark Report underscored many of the challenges in compliance programs today—they are reactive, and employees find them stressful and lacking strategy and efficient resourcing. And yet, compliance can support business growth through new business, better controls, and improved risk management.

Based on the key takeaways above, we suggest the following best practices to make your compliance program more strategic and less onerous.

Compliance can support business growth.

1. Create a Master Audit Plan

We noted earlier that compliance is all too often reactive and not proactive. Driven by external requests, organizations scramble to perform an audit under pressure. When this happens multiple times for multiple frameworks, organizations find themselves in a near-permanent state of chaos.

We advise organizations to step back from the whirlwind of their daily activity and create a master audit plan.

Take a look at what your organization is already pursuing, assess the requirements of various certifications or reports, and determine your company's future audit needs in advance.

For example, organizations extending a line of business to U.S. federal agencies may need to pursue Federal Risk and Authorization Management Program (FedRAMP) authorization or Federal Information Security Management Act (FISMA) certification. Companies looking to work with patient data in the U.S. may need to comply with the Healthcare Insurance Portability and Accountability Act (HIPAA).

Once your organization understands the current audits underway and the future landscape, you can:

- Lay out the milestones quarter over quarter and year over year
- Create a rhythm that works for everyone
- Implement shared processes
- Communicate the value of audits across the organization

All of these elements come together in a master audit plan.

2. Consolidate Audits (and Auditors)

Part of creating a master audit plan is to consolidate audits. For organizations pursuing multiple audits, it's likely that much of the data and evidence will overlap.

Consolidating audits onto a single timeline can greatly ease the disjointedness of auditing. Instead of responding to the same request for data several times, IT and cybersecurity teams can provide data more efficiently. And because the audit is strategically planned and expected, it becomes less of a last-minute scramble.

Of course, this may mean a change in partners, too. As we found in this report, organizations work with different auditors across multiple audits. This can lead to inefficiencies, added costs, and disparate processes. When you consolidate audits, look to consolidate auditors, too—and find a true partner who can grow with your business goals and master audit plan.

It can take a few years to consolidate audits, and organizations must be careful not to fall into "gaps" in compliance. However, the effort of consolidating audits (and auditors) has enormous benefits.

3. Establish Strong Communication and Collaboration

As we found in this year's survey, organizations struggle with staffing and tedious data collection, and preparing for an audit or assessment eats up months of their time. These constraints create the perfect conditions for miscommunication and mistakes.

Thinking of auditing as a year-round process (rather than something to be done one to two months before the audit) is one of the best ways to improve the process and create strong channels of communication.

Organizations can make auditing easier by building a clear process, defining roles, and coordinating communication. Steps can include:

- Appointing a compliance project manager (or team), either for an individual audit or for all audits
- Establishing a calendar of must-do controls and to-dos
- Assigning items on the calendar to specific members of IT, cybersecurity, etc.
- Conducting regular check-ins to ensure these action items have been met
- Collecting evidence throughout the year
- Touching base regularly throughout the year on audit processes and next steps

When organizations build compliance activities into their culture, the prep time needed will be much shorter when the audit comes due.

4. Invest in Technology for Efficiency

As we found in our survey, very few companies tap into technology for their compliance process. Yet software—which has transformed and streamlined so many other aspects of business—can be a powerful tool for making audits more efficient.

The best compliance programs are year-round efforts—not heroic last-minute pushes. With technology that includes workflow management and collaboration tools, organizations can put in place processes to collect evidence on time.

A good compliance software platform can:

- Enable better communication between teams
- Centralize evidence
- Organize information as it is collected/added
- Deduplicate evidence
- Assign evidence to multiple overlapping audits where applicable

When organizations are proactively organized, auditors are better able to do their job. There are far fewer ad hoc questions about evidence and gaps in information. Good compliance management software can also streamline communications with compliance consultants and experts, which can save time during audit preparation.

5. Choose a Long-Term Partner

A small software company can quickly become a global phenomenon, while a new client can help you expand into new industries. While these types of changes are exciting, they also come with increased compliance and regulatory needs.

There are different approaches to handling this increased need for compliance. Some organizations like to work with auditors on a more transactional level—they come in, do an audit, and leave. Others prefer to work with one auditor for decades. Both approaches have their merits and drawbacks, depending on an organization's goals. Still, we see greater benefits from selecting a long-term partner with the right tools and strategic advice to drive your compliance efforts.

The right auditor can be a powerful partner for growth. They should be by your side year-round to advise your organization on certifications and assessments—not just at audit time. They should also operate globally in the markets that matter to you and provide insights into the compliance horizon, which is more important than ever in the face of rising privacy regulations and cybersecurity threats.

When you consider consolidating auditors, look for a true partner who can grow with you.

The right auditor can be a powerful partner for growth.

Compliance in Service of Business Growth and Security

As they stand, many compliance programs present real resourcing and workflow issues to companies—but it doesn't have to be this way.

Compliance drives your business. The right combination of audits, assessments, or certifications demonstrates business maturity and cybersecurity savvy to your customers, partners, and other stakeholders. Most of all, it builds trust.

With this report's results in hand, we encourage all organizations to make 2021 the year they embrace new processes, strategies, and automation technologies to grow, reduce risk, and achieve ambitious goals

A-LIGN uniquely delivers a single-provider approach as a licensed SOC 1 and SOC 2 Assessor, accredited ISO 27001, ISO 27701 and ISO 22301 Certification Body, HITRUST CSF Assessor firm, accredited FedRAMP 2PAO, designated CMMC C3PAO, and Qualified Security Assessor Company. Working with small businesses to global enterprises, A-LIGN experts and its proprietary compliance management platform, A-SCEND, are transforming the compliance experience.

For more information, visit www.A-LIGN.com.

Special Thanks

We thank our respondents for candidly sharing their compliance program experiences. We also thank Eagle Certification Group in particular for their valuable contributions to this report.